Defense Department Proposal to Establish the RESTRICTED Classification

Loss of U.S. technology is pervasive and uncontrolled. The unremitting flow of unclassified national security information to hostile nations, particularly technology and technical data with military application, is one of the more serious problems confronting this Administration. There is ample evidence that Soviet bloc acquisitions of unclassified national security related publications poses a considerable threat to the U.S. military posture and that of our allies. It greatly enhances our adversaries' capabilties to design, produce and field weapons systems of all types, as well as develop measures to counter U.S. weapons systems. It cuts their production costs, shortens their production times, and improves the quality of their product.

A Soviet scientist who defected several years ago told Congress that the majority of Soviet information collection requirements can be openly obtained in the United States. The FBI has estimated that as high as 90% of the Soviet collection requirements can be satisfied through open sources. We are painfully aware of Communist bloc efforts within the United States to obtain technology, most of which through legal means, which we are powerless to stop. Prior to February 1980, for example, we stood helplessly by as the Soviet Union purchased 80,000 technical documents each year from the National Technical Information Service (NTIS). Although their access to the NTIS has now been officially terminated, their surrogates continue to exploit this source of extremely valuable information.

Members of Congress, industry spokesmen, and the media frequently lament this state of affairs, and ask is there nothing that can be done. Unfortunately it has always been presumed that little could or should be done to limit such acquisitions, relying instead on the ability of the originators of such documents to properly secure sensitive information by using the existing security classification system. This is precisely the point of the Defense proposal. The existing three-level classification scheme has not provided adequate protection to a large body of sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of our Armed Forces.

Classification of such information under the current three-level system has been neither possible nor practical. Although such sensitive national security information fits the categories permitted to be classified, it does not rise to the level of the "identifiable damage" standard prescribed by the current Order, nor does it rise to the "damage" standard of the draft revision. Disclosure of the technical characteristics of electronic components used in a missile guidance system, for example, may not appear to damage the national security, and yet may well provide our adversaries with precisely what they need to produce a more effective missile. It is this "damage" standard that is applied

by orginators in deciding whether to make their documents unclassified or to protect them by security classification.

At the practical level, there is also need to permit defense components, contractors, and other government entities to freely utilize and exchange information of this nature without the costs and delays entailed by safeguarding requirements imposed under the current three-level system. Using the previous example, if the technical characteristics of the electronic components were classified under the provisions of the present Order, no one could handle them or have access to them without a security clearance; they could not be stored or transmitted except by approved means; and they could not be discussed except over secure communications. Under the current system of classification, technical information of this sort is frequently not classified because the owner of the information believes his need to freely utilize it takes precedence over whatever advantage the United States might lose if the information were disclosed to our adversaries. He might well be right, but the legal consequence of his decision is to make the information available under a variety of circumstances such as the Freedom of Information Act; through government distribution centers; discussion in industry marketing brochures, presentations, and meetings; through the Federal Depository Library System; through the International Exchange Program; speeches; cultural and trade exchanges.

It is to remedy this situation -- to make possible control over dissemination of technical information without at the same time creating a system that would unduly inhibit the defense industrial process -- that DoD has proposed the fourth level of classification. It would allow us, and other agencies, to classify information useful to our adversaries, enabling us to keep it out of public dissemination channels while at the same time subjecting it to minimal controls within the federal government and defense industry communities. As we conceive it, the only requirement for access to RESTRICTED would be a legitimate need for it in the performance of official government functions. No background investigation would be required prior to granting access. Storage and handling requirements would similarly be minimal to prevent persons who had no official need for the information from obtaining access to it.

Some may argue that a fourth level of classification would dilute the efficacy of the security classification system resulting in a loss of its credibility. Quite the contrary, the fourth classification level strengthens the system by authorizing the protection of valuable national security information that is now jeopardized because "nothing can be done about it under the current Order. It recognizes a serious information control problem and provides a credible solution. The "damage" standard remains undiluted for the higher levels of classification; the fourth classification level introduces a realistic "loss" standard for the protection of sensitive national security information that is now unprotected; and the overall classification protection of information in the interest of national security is strenghtened. Expansion of the current classification scheme will not be viewed as a radical departure

but rather as a reasonable, necessary, and responsible extension of access controls over information based on legitimate security concerns.

Most of the NATO member nations and NATO itself use a four-level security classification system to include the classification "Restricted." The incompatibility of the U.S. three-level system with NATO and many countries outside of NATO continually creates operational problems having an adverse effect on NATO interoperability and standardization. These and other persistent problems would be resolved with the establishment of "Restricted" as a U.S. security classification.

Alternatives put forth to accomplish such increased controls, such as amending the FOIA or existing statutes governing export control fail to recognize the duty and authority to protect national security information which clearly resides with the President.

Other alternatives, such as increased emphasis on dissemination control systems by individual agencies or through additional Executive orders, do not have the force or immediate effect of security classification. Nor would such controls, under existing legislative policy, be sufficient to effectively stem the flow of sensitive national security information to hostile nations.

We want to make clear this additional category of classification is not intended to preclude any greater public awareness of defense activities, operations or policy than is now possible. We emphasize our purpose is solely to protect certain information by subjecting its dissemination through open channels to greater control. We want to deny our adversaries the proverbial "silver platter" they now have. Private firms and individuals in the United States who need this information to continue to do business with the Government will continue to get it, but through official channels rather than sources available to the general public.

It is my understanding that other Executive Branch agencies are reluctantly distributing and releasing information that is disadvantageous to U.S. national security interests. It was for this reason that we included in our proposed definition of Restricted loss of a "diplomatic" or "intelligence" advantage. However, if State and CIA do not share the same degree of concern over loss of such information as we do over military technology and operational information then we would offer the following more narrow definition for Restricted information as an alternate proposal:

> "Restricted" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the United States of a technological or military advantage and which requires protection in the interest of national security.

This alternately defined fourth classification level would apply to a wide range of technical and training data produced by this Department

which does not meet the current criteria for classification. This information, invaluable as a reflection of the state-of-the-art of military technology and the extent to which it has tactical and strategic military application is highly sought and easily obtained by our adversaries. Several highly classified studies can be provided that demonstrate the degree to which our adversaries are using such information to their immediate and long-range benefit. However, the benefit of the alternative proposal principally accrues to this Department since it is the primary and largest user of technology related and military operational information.

The current uncontrolled dissemination of sensitive but unclassified national security information, especially when taken in the aggregate, is demonstrably disadvantageous to U.S. national security interests. The loss of such information and the advantages gained by our adversaries requires that steps be taken now to provide legal and positive control of it. We continue to urge approval of our initially proposed fourth level of classification as an effective and inexpensive means to restrict access to sensitive national security information that is now unprotected. While we would accept the proposed alternate, more narrow definition that ameliorates some of this Department's concerns, we continue to believe that the problem of inadequate protection of sensitive national security information extends throughout the Executive Branch. There are no other acceptable alternatives if we are to discharge effectively our considerable responsibility for the protection of information in the interest of national security.

Changes to the revised order necessary to establish the RESTRICTED classification are as follows:

Change Section 1-101 to read:

> 1-101. National security information...shall be classified at one of the following [three] four levels:

Add Section 1-101(d) to read:

> 1-101(d). "Restricted" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the United States of a technological, diplomatic, intelligence, cryptologic, or military advantage and which requires protection in the interest of national security.

Change Section 1-302 to read:

> 1-302. Information...shall be classified when...its unauthorized disclosure reasonably could be expected to cause the loss of an advantage to the United States or cause damage to the national security.

Change Section 1-501(d) to read:

(d) one of the [three] four classification designations....

Change Section 4-101 to read:

4-101. A person is eligible for access to Restricted information only when such access is essential to the accomplishment of authorized and lawful Government purposes. A person is eligible for access to [classified] Top Secret, Secret, or Confidential information only after a [formal] favorable determination of trustwothiness....